CERT® Advisory CA-2003-09 Buffer Overflow in Microsoft IIS 5.0

Original issue date: March 17, 2003
Last revised: Mon Mar 17 14:34:35 EST 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Windows 2000 with IIS 5.0 enabled

Overview

A buffer overflow vulnerability exists in Microsoft IIS 5.0 running on Microsoft Windows 2000. IIS 5.0 is installed and running by default on Microsoft Windows 2000 server products. This vulnerability may allow a remote attacker to run arbitrary code on the victim machine.

An exploit is publicly available for this vulnerability, which increases the urgency that system administrators apply a patch.

I. Description

IIS 5.0 includes support for WebDAV, which allows users to manipulate files stored on a web server (RFC2518). A buffer overflow vulnerability exists in ntdll.dll (a portion of code utilized by the IIS WebDAV component). By sending a specially crafted request to an IIS 5.0 server, an attacker may be able to execute arbitrary code in the Local System security context, essentially giving the attacker compete control of the system.

Microsoft has issued the following bulletin regarding this vulnerability:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-007.asp

This vulnerability has been assigned the identifier CAN-2003-0109 by the Common Vulnerabilities and Exposures (CVE) group:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109

II. Impact

Any attacker who can reach a vulnerable web server can gain complete control of the system and execute arbitrary code in the Local System security context. Note that this may be significantly more serious than a simple "web defacement."

III. Solution

Apply a patch from your vendor

A patch is available from Microsoft at

http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&displaylang=en

Disable vulnerable service

Until a patch can be applied, you may wish to disable IIS. To determine if IIS is running, Microsoft recommends the following:

Go to "Start | Settings | Control Panel | Administrative Tools | Services". If the "World Wide Web Publishing" service is listed then IIS is installed

To disable IIS, run the IIS lockdown tool. This tool is available here:

http://www.microsoft.com/downloads/release.asp?ReleaseID=43955

If you cannot disable IIS, consider using the IIS lockdown tool to disable WebDAV (removing WebDAV can be specified when running the IIS lockdown tool). Alternatively, you can disable WebDAV by following the instructions located in Microsoft's Knowledgebase Article 241520, "*How to Disable WebDAV for IIS 5.0*":

http://support.microsoft.com/default.aspx?scid=kb;en-us;241520

Restrict buffer size

If you cannot use either IIS lockdown tool or URLScan, consider restricting the size of the buffer IIS utilizes to process requests by using Microsoft's *URL Buffer Size Registry Tool*. This tool can be run against a local or remote Windows 2000 system running Windows 2000 Service Pack 2 or Service Pack 3. The tool, instructions on how to use it, and instructions on how to manually make changes to the registry are available here:

URL Buffer Size Registry Tool - http://go.microsoft.com/fwlink/?LinkId=14875
Microsoft Knowledge Base Article 816930 -

http://support.microsoft.com/default.aspx?scid=kb;en-us;816930
Microsoft Knowledge Base Article 260694 -
http://support.microsoft.com/default.aspx?scid=kb;en-us;260694

You may also wish to use URLScan, which will block web requests that attempt to exploit this vulnerability. Information about URLScan is available at:

http://support.microsoft.com/default.aspx?scid=kb;[LN];326444

Appendix A. Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Microsoft Corporation

Please see Microsoft Security Bulletin MS03-007.